**Incident handler's journal**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

|  |  |
| --- | --- |
| **Date:**  8/9/25 | **Entry:**  1 |
| Description | U.S. health care clinic phishing incident malicious attachment downloading ransomware and encrypting organization’s computer files. |
| Tool(s) used | None |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: Unethical hacker group * **What**: phishing attack successfull and downloaded ransomware * **When**: Tuesday 9:00 a.m. * **Where**: U.S. health care clinic computers * **Why**: Someone followed malicious attachment sent by phishing attack and ransomware was forcefully downloaded. |
| Additional notes | I wonder what the phishing email looked like for an employee to find it believable enough to click on it, or if it was just negligence. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:**  2 |
| Description | Employee opened a protected file and had a malicious payload downloaded onto computer. |
| Tool(s) used | OSINT VirusTotal |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: Unknown * **What**: Phishing attack with malicious attachment downloaded and seems to be malware that downloaded malicious payload onto employee’s computer. * **When**: Unknown * **Where:** Employee’s computer * **Why**: Employee followed malicious attachment from phishing attack, downloaded malicious file. |
| Additional notes | Maybe more training on determining what is a phishing attack needs to be done for the employees. Also the file was determined to be malware. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:**  3 |
| Description | Investigating alert ticket of potential successful phishing attack |
| Tool(s) used | None |
| The 5 W's | * **Who**: Unknown malicious actor with email 76tguyhh6tgftrt7tg.su * **What**: Employee sent phishing email with malicious attachment to download file, when password entered a malicious payload was dumped onto computer. * **When**: Wednesday, July 20, 2022 09:30:14 AM * **Where**: Employee’s computer * **Why**: Employee fooled by phishing email into downloaded attachment, opened malware. |
| Additional notes | Phishing alert is legitimate as email is convoluted, sender IP is strange, attached file is an executable which is strange for a “resume”, and grammatical errors in body of email. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:**  4 |
| Description | Unknown malicious actor performed forced browsing attack on e-commerce web application by modifying order number to gain PII from customers. |
| Tool(s) used | None |
| The 5 W's | * **Who**: Unknown actor * **What**: Forced browsing attack on e-commerce applications causing estimated financial loss of $100,000 and estimated breach of 50,000 affected customers’ PII. This attack went unnoticed until it was reported by employee receiving ransom emails from attacker for money in exchange for breached data. * **When**: December 28, 2022, at 7:20 p.m., PT * **Where:** E-commerce web application * **Why**: Vulnerability in e-commerce web application allowing malicious actors to perform a brute force attack abusing the order number in the URL to receive PII from customers. |
| Additional notes | Vulnerability has been patched, and public relations department was contacted to disclose the situation to affected customers. Further investigation of logs showed that a large volume of sequentially listed customer orders was used, indication of the brute force attack. Precautions for the future include performing routine vulnerability checks, setting a URL request range, and allowing only authenticated users to access content. |